DETEKSI PAKET SCANNING PADA SISTEM KEAMANAN JARINGAN BERBASIS LINUX KERNEL 2.4.X.X

Setia Juli Irzal[1], Agus Virgono Ir Mt ; Gunawan Adi St[2], [3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Kata Kunci :

Abstract

Keywords :

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan data dalam sebuah jaringan seringkali merupakan hal yang terabaikan. Seoranga penyusup umumnya dapat dengan mudah memasuki sebuah jaringan tanpa harus melewati sebuah firewall. Seorang penyusup akan melakukan penyelidikan terlebih dahulu terhadap sistem keamanan dari jaringan komputer target, sebelum dia berusaha mendapatkan akses pada jaringan tersebut Bila ternyata jaringan komputer tersebut memiliki sistem keamanan yang lemah, maka penyusup melakukan serangan dan berusaha mendapatkan akses pada jaringan tersebut. Tapi bila ternyata jaringan tersebut memiliki sistem keamanan yang baik, maka penyusup akan berpikir dua kali sebelum berusaha masuk.

Dari uraian diatas terlihat bahwa proses pengumpulan informasi sistem keamanan, merupakan langkah awal yang harus dilakukan oleh seorang penyusup sebelum melakukan serangan. Paket scanning merupakan langkah yang tepat untuk mengetahui konfigurasi sebuah jaringan. Setelah mengetahui konfigurasi sebuah jaringan, barulah kemudian didapatkan celah-celah untuk melakukan serangan terhadap jaringan tersebut. Untuk itulah seorang administratur jaringan harus dapat mengetahui karakteristik dari paket scanning ini sehingga kemudian dapat melakukan deteksi terhadap paket scanning, dan kemudian dapat dilakukan tindakan pengamanan untuk mencegah terjadinya kerusakan pada sistem informasi.

1.2 Perumusan Masalah

Semakin berkembangnya metoda scanning yang digunakan oleh penyusup membuat alat bantu deteksi scanning semakin sulit untuk melakukan deteksi paket scanning. Sehingga harus selalu dilakukan pengembangan dan pendefinisian ulang terhadap parameter parameter deteksi paket scanning.

Pada tugas akhir ini akan dicoba dilakukan percobaan packet scanning, agar kemudian dapat dipelajari dan dilakukan definisi terhadap parameter-parameter deteksi paket scanning

1.3 Batasan Masalah

Agar pembahasan dalam tulisan ini menjadi jelas dan terarah, maka terlebih dahulu ditentukan batasan masalah yaitu, pembahasan difokuskan pendefinisian parameter-parameter deteksi paket scanning. Sistem operasi yang digunakan pada jaringan dibatasi pada Linux kernel 2.4.x.x

1.4 Tujuan Penulisan

Tujuan penulisan ini adalah mempelajari metoda paket scanning detection, membuat aturan-aturan parameter-parameter IP header yang digunakan dalam penentuan deteksi paket scanning pada linux kernel 2.4.x.x

1.5 Metodologi Penelitian

Dalam penyelesaian tugas akhir ini dilakukan studi secara komprehensif dan komparatif. Hal pertama yang dilakukan adalah studi literatur dengan mengumpulkan data melalui buku, majalah, dan jurnal-jurnal ilmiah yang berkaitan dengan paket scanning. Setelah mendapatkan gambaran yang jelas tentang konsep-konsep di atas, maka dilakukan percobaan dan simulasi paket scanning pada jaringan komputer berbasis Linux Kernel 2.4.x.x. Setelah didapatkan data hasil simulasi maka dilakukan analisa serta pendefinisian terhadap parameter-parameter deteksi paket scanning.

1.6 Sistematika Penulisan

Sistematika penulisan dalam tugas akhir ini disusun dalam lima bab, yang secara garis besar adalah sebagai berikut :

BAB I **PENDAHULUAN**

Berisi uraian mengenai latar belakang, perumusan masalah, pembatasan masalah, tujuan penulisan dan metodologi penelitian

BAB II **LANDASAN TEORI**

Menjelaskan secara singkat tentang security dalam jaringan, khususnya tentang packet scanning

BAB III **SIMULASI PAKET SCANNING**

Melakukan simulasi packet scanning, mengumpulkan data

packet scanning

BAB IV ANALISA DETEKSI PAKET SCANNING

Melakukan analisa terhadap data hasil paket scanning dan melakakun definisi terhadap parameter-parameter deteksi paket scanning.

BAB V KESIMPULAN DAN SARAN

Bab ini mengemukakan kesimpulan dari tugas akhir ini dan saran-saran dari penulis untuk pengembangan lebih lanjut

BAB V
PENUTUP

5.1 Kesimpulan

Paket scanning merupakan sebuah aktifitas yang harus diawasi secara ketat, karena bila dilakukan oleh seorang penyusup yang handal, maka akan sangat mudah didapatkan lubang-lubang keamanan dari sebuah jaringan. Pendeteksian aktifitas scanning harus disesuaikan dengan metoda scanning yang digunakan. Dari hasil percobaan terlihat metoda scanning konvensional dapat dengan mudah kita definisikan parameternya. Hanya saja beberapa metoda lanjutan pendefinisian parameter agak sedikit sulit, sehingga pendeteksian memerlukan pengamatan log jaringan secara baik.

Untuk melindungi keamanan data dari jaringan sebaiknya dilakukan pemfilteran terhadap protokol ICMP. Walaupun begitu tindakan ini akan menyulitkan administratur jaringan dalam melakukan proses pemeliharaan secara remote.

5.2 Saran

Berkurangnya kenyamanan merupakan sebuah harga yang harus dibayar demi meningkatkan keamanan sebuah jaringan. Pembatasan terhadap paket scanning merupakan hal yang mutlak harus dilakukan. Disinilah peran seorang administrator jaringan mutlak dibutuhkan. Untuk meningkatkan fungsi pengawasan terhadap paket scanning dan mengurangi human error, sebaiknya dikembangkan alat bantu pemfilter paket yang bersifat adaptif berbasis sistem kecerdasan artificial yang tidak hanya mampu menganalisa tapi juga secara real time melakukan respon secara tepat

DAFTAR PUSTAKA

[1] Onno W. Purbo, Adnan Basalamah, Ismail Fahmi, Achmad Husni Thamrin, *"TCP/IP: Standar, Desain, dan Implementasi"*, Elex Media Komputindo, Desember 1999.

[2] William Stallings, "*Data &Computer Communications*", Prentice Hall 6th Edition,2000

[3] Stephen A. Thomas, *"IP Switching and Routing Essentials: Understanding RIP, OSPF, BGP, MPLS, CR-LDP, and RSVP-TE"*, hal. 25-46, John Wiley & Sons, Inc., 2002.

[4] RFC 1244, P. Holbrook (CICNet)J. Reynolds (ISI),"*Site Security Handbook*", IETF,July 1991

[5] RFC 1256, S. Deering-Xerox PARC,"*ICMP Router Discovery Messages*", IETF September 1991

[6] RFC 1349, P. Almquist, "*Type of Service in the Internet Protocol Suite*",IETF July 1992

[7] RFC 2521, P. Karn- Qualcomm, W. Simpson-DayDreamer, "ICMP Security Failures Messages" IETF March 1999